TRABAJO FIN DE GRADO

GRADO EN INGENIERÍA INFORMÁTICA

CURSO 2015-2016

INTEGRIDAD EN IMÁGENES DE DISPOSITIVOS MÓVILES

SANTIAGO GÓMEZ MUÑOZ

Directores:

Luis Javier García Villalba

Ana Lucila Sandoval Orozco

Departamento de Ingeniería del Software e Inteligencia Artificial

---

FACULTAD DE INFORMÁTICA

UNIVERSIDAD COMPLUTENSE DE MADRID

El presente Trabajo Fin de Grado se enmarca dentro de un proyecto de investigación titulado RAMSES aprobado por la Comisión Europea dentro del Programa Marco de Investigación e Innovación Horizonte 2020 y en el que participa el Grupo GASS del Departamento de Ingeniería del Software e Inteligencia Artificial de la Facultad de Informática de la Universidad Complutense de Madrid (Grupo de Análisis, Seguridad y Sistemas, http://gass.ucm.es, grupo 910623 del catálogo de grupos de investigación reconocidos por la UCM).

Por razones de confidencialidad del proyecto se ha omitido información del trabajo desarrollado para no infringir la normativa correspondiente.

_____

Santiago Gómez Muñoz

_____ _____

Luis Javier García Villalba Ana Lucila Sandoval Orozco

Agradecimientos

Primero, quisiera agradecer a Luis Javier García Villalba y a Ana Lucila Sandoval Orozco, los Directores de este Trabajo, todo el apoyo que me han proporcionado para la realización de este trabajo.

Segundo, me gustaría agradecer los miembros de mi familia, a mis padres y hermanos que me han mostrado su apoyo y ánimos durante la creación de este trabajo así como la oportunidad de poder realizar el Grado de Ingeniería Informática.

Por último, quisiera agradecer a todos aquellos equipos de desarrolladores que han desarrollado las herramientas y documentación necesarias para la comunidad y que han servido como soporte para la realización de este trabajo.

Resumen

El presente trabajo trata de dar respuesta al problema de verificación de manipulación de imágenes digitales obtenidas con los dispositivos móviles. La inmensa cantidad de información digital que nos rodea dificulta enormemente poder verificar su autenticidad. Este problema, unido a la falta de pensamiento crítico, ha provocado que tendamos a aceptar como verdadero todo lo que vemos, sin cuestionar siquiera la legitimidad de dicha información. Lo que permite que uno sea fácilmente manipulable a voluntad de aquellos que buscan mediante dicho engaño obtener un beneficio. Por ello, la principal motivación de este trabajo es tratar de minimizar su impacto, creando una herramienta que realiza un estudio de imágenes digitales que permita obtener un rápido resultado y verifique la autenticidad de esta información. Para ello el sistema propuesto extrae las tablas de cuantificación de las imágenes para posteriormente ser analizadas y dar un veredicto sobre la imagen analizada. Esta herramienta no sólo tiene en cuenta la manipulación de la información almacenada en una imagen obtenida mediante un dispositivo digital, sino también aquella que ha sido manipulada mediante los más conocidos programas de edición de imágenes para ampliar su espectro y conseguir una mejor tasa de detección y una reducción de los falsos positivos, consiguiendo así un método de bajo coste en recursos y tiempo.

Palabras clave

Dispositivos Móviles, Exif, Falsificación, Manipulación de Imágenes, Tablas de Cuantificación, Verificación.

Abstract

The present work tries to give an answer to the recent problem of image verification of manipulated images obtained by mobile devices. We are surrounded by a big extent of digital information, which makes authenticity a great problem. This problem, and the lack of critical thought, made us to accept as true everything we see, without ever questioning the legitimacy of such information. This allows us to be easily manipulated at will, by those who seek to make a profit in that deception. Therefore, the main motivation of this work, is to try to minimize its impact; by creating a tool that performs a study of digital images to obtain a quick result and verify the authenticity of this information. With this focus in mind, the proposed system extracts the quantization tables of images to be analysed subsequently and give a verdict over the analysed image. This tool not only takes into account the manipulation of the information stored in an image obtained by a digital device, but also the one that has been manipulated by the most popular programs of image manipulation to expand its spectrum and get a better detection rate and a reduction in the false positives, achieving a framework with a low-cost of resources and time.

Keywords

Exif, Falsification, Image Manipulation, Mobile Devices, Quantization Tables, Verification.

Lista de Acrónimos

APP	Applitation Marker
BBDD	Base de datos
CCD	Charged-Coupled Device
CFA	Color Filter Array
CMOS	Complementary Metal-Oxide Semicondutor
CMYK	Cyan, Magenta, Yellow, Key
CSC	Compact System Camera
DHT	Define Huffman Table
DQT	Define Quantization Table
DRI	Define Restart Interoperability
DSLR	Digital Single Lens Reflex
DWT	Discrete Wavelet Transform
DyWT	Undecimated Dyadic Wavelet Transform
EOI	End Of Image
EXIF	EXchangeable Image file Format
FPS	Frames Per Second
HD	High Definition
HOGM	Histogram of Oriented Gabor Magnitude
HSL	Hue, Saturation Lightness
LED	Light Emitting Diode
MP	Megapixel
PDA	Personal Digital Assistant
PRNU	Photo Response Non-Uniformity

RGB	Red, Green, Blue
RMS	Root Mean Square
RYB	Red, Yellow, Blue
SMS	Short Message System
SOF	Start Of Scan
SOI	Start Of Image
SPN	Sensor Pattern Noise
sRGB	RGB Standard
STS	Sentencia del Tribunal Supremo
VGA	Video Graphic Array

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

1.1. Motivación

La popularización de las cámaras en los teléfonos móviles ha provocado una revolución en el mundo de la fotografía. Esto ha traído una gran serie de ventajas pero también varios inconvenientes. Los teléfonos móviles han puesto al alcance de los apasionados de la fotografía, un medio accesible para iniciarse en este mundo, sin embargo, ha provocado un aumento increíble en el número de contenidos digitales así como de la calidad de estos. En el entorno en el que vivimos, se ha producido un exceso de información, esto permite ser una generación más informada pero no se disponen de los mecanismos necesarios para procesarla y filtrar los elementos no deseados. Debido a esto se ha perdido nuestra capacidad de pensamiento crítico, aceptando cualquier información obtenida como verdadera sin cuestionar su origen.

La tecnología de las cámaras de los teléfonos móviles sigue mejorando y aumentando sus prestaciones, aunque la cámara compacta, o réflex, seguirá manteniendo su uso en los segmentos más profesionales. Las cámaras móviles han puesto en serios aprietos a las compactas, pero aún no han logrado desplazar a las DSLR (del inglés Digital Single Lens Reflex) o una buena CSC (del inglés Compact System Camera). La fotografía móvil tiene usa serie de ventajas respecto a las cámaras tradicionales, sobre todo la instantaneidad de las fotografías, pues no siempre se cuenta con una cámara réflex, pero siempre se cuenta con el teléfono móvil, además las compactas encajan mejor cuando se quiere fotografiar algún elemento con mayor calidad o características. Ambas tecnologías pueden convivir y su diferencia se basa en las características que se desean obtener a la hora de hacer la captura. La importante es capturar el momento, sin importar el medio [1].

Las mejoras en el segmento de la tecnología de los teléfonos móviles; mejores cámaras, nuevas pantallas, conexión a Internet…, ha provocado un cambio en la forma de trabajar de muchos profesionales. Gracias a Internet y las mejoras de estas tecnologías han convertido a estos dispositivos en verdaderos centros multimedia, ocio y comunicación. Dentro del ámbito del Periodismo ha democratizado y mejorado su difusión. Gracias a los móviles, los comunicadores han pasado por una gran serie de cambios como, la posibilidad de obtener imágenes captadas por los propios usuarios, por ejemplo, las protestas en la primavera Árabe, y también la estandarización del periodista orquesta, donde el redactor debe ser capaz de además de redactar la noticia, encargarse de otros elementos como la inclusión de sus propias imágenes y vídeos [1].

Sin embargo, surgen dudas sobre la validez que pueden tener los mensajes de WhatsApp, fotos, SMS y demás contenido presente en un Smartphone, Tablet, entre otros dispositivos móviles. La respuesta es variable y necesita un análisis de cada caso. Lo que sí se puede afirmar es que dicho contenido es perfectamente válido como prueba en un procedimiento judicial, siempre y cuando, a la hora de obtener dicha prueba los derechos fundamentales sean respetados. Una vez garantizado esto, es necesario analizar hasta qué punto es suficiente dicha prueba, especialmente en el proceso penal demostrar la inocencia o culpabilidad un acusado penal respaldado por el principio de presunción de inocencia.

Para que una prueba pueda ser considerada y provocar una condena pena es necesario que cumpla una serie de propiedades. La primera, el origen de la prueba es fundamental, es decir, solo tendrá validez, aquella prueba obtenida mediante la orden de un juez y que esta sea facilitada por la propia empresa que "almacena" los datos (Twitter, Facebook, etc.), no obstante, si la prueba es facilitada por el propio denunciante, es necesario que esta disponga de una serie de elementos para comprobar su veracidad. Esto se debe a la facilidad con

que dichas pruebas puedan ser modificadas, como borrar algún elemento no deseado de la imagen, también es posible que otra persona, haya interceptado la comunicación o dispositivo móvil para suplantar la identidad del usuario o que simplemente dichas pruebas hayan podido ser modificadas por un técnico informático.

Según STS 1415/ 2003, del 29 de Octubre, el derecho a la presunción de inocencia del art. 24.2 CE exige al Tribunal de instancia lo siguiente:

- Que exista una prueba con un contenido de cargo.
- Que dicha prueba de cargo haya sido obtenida y aportada al proceso siguiendo las normas de la Constitución y de la Ley procesal.
- Que la prueba de cargo sea razonable y considerada como suficiente para justificar la condena penal.

Por tanto, cualquier medio de "prueba tecnológica" puede ser utilizado en un procedimiento judicial. Sin embargo, la misma puede no ser suficiente para condenar a un acusado. Así, utilizar cualquier medio de prueba disponible es tan importante como, demostrar que dichos medios de prueba, tengan validez suficiente para conseguir una condena penal. Para conseguirlo, es fundamental que dicha prueba haya sido obtenida por la autoridad judicial correspondiente o que esté avalada por una pericial informática. De ahí la importancia del análisis forense de imágenes digitales de dispositivos móviles en la actualidad. En [2] se presenta un estudio sobre la necesidad de la existencia de técnicas de análisis forense específicas para dispositivos móviles.

1.2. Contexto

El presente Trabajo Fin de Grado se enmarca dentro de un proyecto de investigación titulado RAMSES aprobado por la Comisión Europea dentro del Programa Marco de Investigación e Innovación Horizonte 2020 (Convocatoria H2020-FCT-2015, Acción de Innovación, Número de Propuesta: 700326)y en el que participa el Grupo GASS del Departamento de Ingeniería del Software e Inteligencia Artificial de la Facultad de Informática de la Universidad Complutense de Madrid (Grupo de Análisis, Seguridad y Sistemas, http://gass.ucm.es, grupo 910623 del catálogo de grupos de investigación reconocidos por la UCM).

Además de la Universidad Complutense de Madrid participan las siguientes entidades:

- Treelogic Telemática y Lógica Racional para la Empresa Europea SL (España)
- Ministério da Justiça (Portugal)
- University of Kent (Reino Unido)
- Centro Ricerche e Studi su Sicurezza e Criminalità (Italia)
- Fachhochschule fur Offentliche Verwaltung und Rechtspflege in Bayern (Alemania)
- Trilateral Research & Consulting LLP (Reino Unido)
- Politecnico di Milano (Italia)
- Service Public Federal Interieur (Bélgica)
- Universitaet des Saarlandes (Alemania)
- Dirección General de Policía - Ministerio del Interior (España)

1.3. Objetivos

El presente Trabajo Fin de Grado (TFG) tiene los siguientes objetivos:

- Realizar un estudio de los trabajos relacionados sobre los tipos de modificaciones posibles en las imágenes para realizar una clasificación de las más relevantes.

- Realizar un estudio de las técnicas de análisis forense de autenticación de imágenes digitales existentes en la literatura con objeto de analizar y comprender las técnicas más relevantes.

- Implementar un algoritmo que permita determinar si una imagen digital ha sido manipulada utilizando los metadatos Exif.

1.4. Plan de Trabajo

El proyecto se ha desarrollado en 3 fases: Definición, Ejecución y Documentación del Proyecto. Las actividades realizadas en cada una de estas fases se presentan en la Tabla 1.1.

Durante la primera fase se establecieron los objetivos y alcance del Trabajo de Fin de Grado, las reuniones con el equipo de tutores y el seguimiento del trabajo realizado durante la elaboración del trabajo. Posteriormente, durante la fase de Ejecución, se desarrolló el proyecto definido en la etapa anterior. Esta fase está compuesta por las siguientes etapas: Especificación de requisitos, diseño, implementación y pruebas. Durante la realización de esta fase, se realizaron actividades de seguimiento y control del avance del proyecto para llevar un control y seguimiento de las actividades realizadas.

Finalmente, en la fase de documentación, se realizó toda la documentación necesaria para la elaboración del Trabajo Fin de Grado. Esta fase se ha realizado en conjunto con las dos fases anteriores.

Nombre de tarea	Duración (días)	Inicio	Fin
• **Definición del proyecto**	**40**	**23/11/15**	**29/01/16**
- Reuniones semanales de seguimiento con los tutores			
- Estudio de los tipos de falsificación de imágenes			
- Estudio de las técnicas de autenticación de imágenes aplicadas a las imágenes obtenidas en dispositivos móviles			
- Definición del proyecto			
• **Ejecución del Proyecto**	**130**	**01/02/16**	**01/07/16**
- Especificación de requisitos			
- Diseño			
- Implementación			
- Pruebas			
- Control			
• **Documentación**	**150**	**14/12/15**	**29/07/16**
- Generación de documentación del proyecto			
- Preparación de la memoria			

Tabla 1.1. Fases del proyecto

1.5. Estructura de la Memoria

El resto del trabajo está organizado en 7 capítulos con la estructura que se comenta a continuación.

En el capítulo 2 se presenta una reseña histórica de la fotografía, el proceso de generación de una imagen de dispositivo móvil, los tipos de sensores utilizados en una cámara de dispositivo móvil y la descripción de los principales sistemas de metadatos en imágenes digitales, dando una especial importancia a la especificación Exif por su alto grado de utilización en los imágenes generadas por dispositivos móviles.

En el capítulo 3 presenta una clasificación de las modificaciones que se pueden realizar sobre una imagen digital según el objetivo de la modificación.

En el capítulo 4 se presentan los trabajos relacionados con las técnicas de autenticación de imágenes digitales.

En el capítulo 5 se especifica una herramienta para el análisis forense de imágenes y vídeos digitales denominada *Theia,* describiendo sus principales características y funcionalidades.

En el capítulo 6 se presenta el algoritmo de verificación de integridad de imágenes propuesto en este trabajo basado en el uso de los metadatos Exif de la imagen. Seguidamente se realiza una evaluación del mismo para analizar su grado de efectividad.

En el capítulo 7 se presentan las principales conclusiones extraídas de este trabajo y las líneas de trabajo futuro.

En los capítulos 8 y 9 se realiza un resumen en inglés de la introducción y las conclusiones del trabajo.

2. IMÁGENES DIGITALES EN DISPOSITIVOS MÓVILES

En los últimos tiempos, uno de los añadidos más importantes en la telefonía móvil ha sido, sin duda alguna, la cámara fotográfica, un dispositivo que ha ido aumentando potencialmente su calidad con el paso del tiempo, mejorando cada vez más el resultado final de las fotografías.

Originalmente, la adición de este componente supuso una especie de añadido meramente presencial, irrelevante a fin de cuentas. Sin embargo, ahora es tan importante que muchos compradores tienen en cuenta este factor a la hora de realizar una nueva adquisición de un dispositivo móvil.

La popularización de las cámaras móviles ha conseguido que la fotografía esté al alcance de la mayoría de la población. Es un elemento esencial que permite la participación; tanto de los profesionales en su trabajo, como de los ciudadanos en su vida cotidiana [3].

2.1. Historia de la Fotografía Móvil

Se considera que la fotografía móvil nació de la mano de Philippe Kahn. Quien envió en Junio de 1977 la imagen de su hija recién nacida. Para ello utilizó su teléfono, una cámara y un ordenador portátil. Siendo el primero en transmitir una imagen por la red de telefonía a unas 2000 personas para mostrarles la foto de hija. Posteriormente, Philippe Kahn trabajó con Motorola en el proyecto para lanzar el primer teléfono con cámara incorporada.

Se considera que ell primer teléfono móvil con cámara incorporada es el *Samsung SCH-V200*, un terminal que se lanzó en Corea del Sur en Junio de 2000 y que contaba con una cámara trasera de 0,35 MP con capacidad de tomar hasta 20 fotografías. No obstante, muchos señalan al *Sharp J-Phone J-SH04* como el primer terminal con cámara fotográfica, que contaba con una cámara de 0,11 MP, sin embargo este no fue lanzado hasta Noviembre de 2000 en Japón. A

diferencia del Samsung, este *Sharp J-SH04*, fue el primer móvil con capacidad de mandar fotografías de forma inalámbrica mediante mensajería. El primer terminal con cámara fotográfica de EE.UU. fue el *Sanyo SCP-5300*, que fue lanzado en Noviembre de 2002, con una cámara de 0,3 MP, una resolución de 640 x 480 píxeles y ajustes personalizables como control de balance de blancos, auto disparador, zoom digital y varios filtros como sepia, blanco y negro, negativo, etc. Después de estos lanzamientos, compañias como Sony Ericsson y Motorola se lanzaron al campo de la fotografía móvil con el *Sony Ericsson P800*, lanzado a finales de 2002 con formato PDA y cámara VGA, y el *Motorola E365* de 2003, con el mismo tipo de cámara VGA.

La primera empresa en lograr el megapíxel de resolución fue Samsung en 2003. La adición de cámaras en los dispositivos móviles fue aumentando y el precio fue cayendo a medida que iban apareciendo nuevos modelos. En Julio de 2004 apareció el *Audiovox PM8920*, con cámara de 1,3 MP y fotos de 1280 x 960 píxeles de resolución. Sony Ericsson lanzó en 2006 su *Sony Ericsson K800i*, con cámara de 3,2 MP y autofocus, estabilizador de imagen y Flash Xenon. Samsung fue la primera en lanzar un terminal con 5 MP en su cámara en 2004 con su modelo *SCH-S250*. Fue en 2007, cuando se lanzó el iPhone original, con una cámara de 2 MP, sin Flash LED, ni autofocus, ni grabación de vídeo. A pesar de todo este avance, fue en 2007 cuando Samsung creó el Samsung *SCH-B600* el primer móvil con cámara de 10 MP, también lanzó en 2007 el *Samsung G800*, el primer móvil con cámara con zoom óptico de 3 aumentos. En 2011, LG y HTC lanzaron al mercado terminales con cámaras 3D, el *HTC EVO 3D* y el *LG Optimus 3D*: que hacían uso de dos cámaras de 5MP para crear imágenes estereoscópicas, que se podían ver en sus pantallas con tecnología 3D sin gafas. No fueron muy populares y debido a sus bajas ventas no se volvieron a lanzar dispositivos con esta tecnología desde entonces.

Inicialmente los Iphone y sus posteriores modelos, no destacaban precisamente por la calidad de imagen en sus cámaras, no fue hasta el modelo

iPhone 4 y gracias a las aplicaciones fotográficas exclusivas de su sistema operativo como Instagram, provoco un aumento de la fotografía móvil social. Tomar una foto en Instagram y subirla a la red se convirtió en un estilo de vida para muchas personas. Desde entonces, se fue popularizando la costumbre de subir fotos de todas nuestras actividades (comida, eventos, viajes) en medios como. El aumento de la calidad en las cámaras móviles y el incremento de usuarios de redes sociales como Twitter o Facebook, plataformas ideales para la publicación de estas imágenes, supusieron un cambio de tendencia. Ahora están importante la cámara de un móvil, que las ventas de cámaras digitales han descendido a mínimos históricos y apenas quedan usuarios que sigan realizando capturas con otros medios que no sea una cámara móvil.

2.2. Proceso de Creación de una Imagen Digital

La fotografía digital se basa en el proceso de capturar la luz y de almacenarla en un medio digital. La principal función de una cámara digital es, por tanto, convertir un rango infinito de niveles de intensidad de luz en una cantidad finita de valores binarios que se almacenará en un medio digital.

La luz entra en la cámara a través del objetivo y llega a la *Matriz de Filtros de Color* (CFA). La matriz CFA es un mosaico de minúsculos filtros de color colocados sobre los píxeles de los sensores de imagen que capturan la información del color. Estos filtros son necesarios porque los fotosensores típicos detectan la intensidad de la luz con poca o ninguna especificidad de la longitud de onda y, consecuentemente, no pueden separar la información del color.

El filtro de Bayer, el más utilizado, se sitúa sobre el sensor digital de imagen para hacer llegar a cada fotodiodo la información de luminosidad correspondiente a una sección de los distintos colores primarios. Interpolando las muestras de cuatro fotodiodos vecinos se obtiene un píxel de color. El

mosaico de Bayer está formado por un 50% de filtros verdes, un 25% de rojos y un 25% de azules. Interpolando dos muestras verdes, una roja y una azul se obtiene un píxel de color.

Después la luz llega a un sensor digital, chip formado por millones de componentes sensibles a la luz que al ser expuestos capturan la imagen fotográfica. En la fotografía digital el sensor electrónico es el equivalente del carrete fotográfico convencional. El sensor es una matriz de elementos fotosensibles que funciona convirtiendo la luz que capta en señales eléctricas que se pueden almacenar, medir y convertir en una representación electrónica del patrón de iluminación que llegó al sensor. Finalmente, el fichero informático que almacena ese patrón puede ser representado en una pantalla de modo que nuestros ojos lo perciban como una imagen.

En la mayoría de cámaras digitales la interpolación cromática se lleva a cabo mediante el software interno de procesamiento de la cámara. La imagen generada por el procesador de imagen se comprime y se almacena en la cámara junto con la información EXIF. Los tipos de formatos de archivos de imagen más comunes son: Formato de imagen sin pérdida de información (RAW, CR2, NEF), formato de imagen comprimida sin pérdida de información (TIFF) y formato de imagen comprimida con pérdida de información que utiliza el estándar de compresión JPEG (JPEG o JPG).

2.3. Tipos de Sensores de una Cámara de Dispositivo Móvil

Los terminales móviles utilizan una tecnología para los sensores de imagen conocida como CMOS (del inglés *Complementary Metal-Oxide Semiconductor*), que es más eficiente que la otra tecnología mayoritaria en sensores, la CCD (del inglés *Charged-Coupled Device*), debido a que tienen un menor consumo de energía, vital en los dispositivos móviles donde cada miliamperio cuenta.

Las mejoras de este tipo de sensores es continua, y ya se pueden conocer los

siguientes avances con los que se podrá contar en el futuro de nuestros dispositivos móviles , como, por ejemplo, el modelo anunciado por OmniVision hace más de un año, el cual tiene un tamaño de 1/2,3 pulgadas y captura vídeos con una calidad de 3840 x 2160 píxeles a 60 fps, es decir, resolución 4K a una velocidad de grabación que duplica la actual (y más usada en vídeo) de 30 fps.

Se dice que el 4k no es el futuro, es el presente, aunque muchos de los lo toman con un cierto escepticismo, de lo que no hay duda es que la resolución 4k –cuatro veces la resolución de Full HD– ofrece posibilidades hasta ahora nunca vistas.

La extracción de fotogramas para obtener una imagen fija de entre 8 y 12 megapíxeles, a partir de un clip de imagen, es la característica que más puede beneficiar a aquellos fotógrafos que se ven obligados a trabajar con varios formatos al mismo tiempo. El 4k ha resuelto una de las mayores dificultades para los profesionales de la imagen: tener que decidir en qué momento se toman fotos y cuando se graba vídeo.

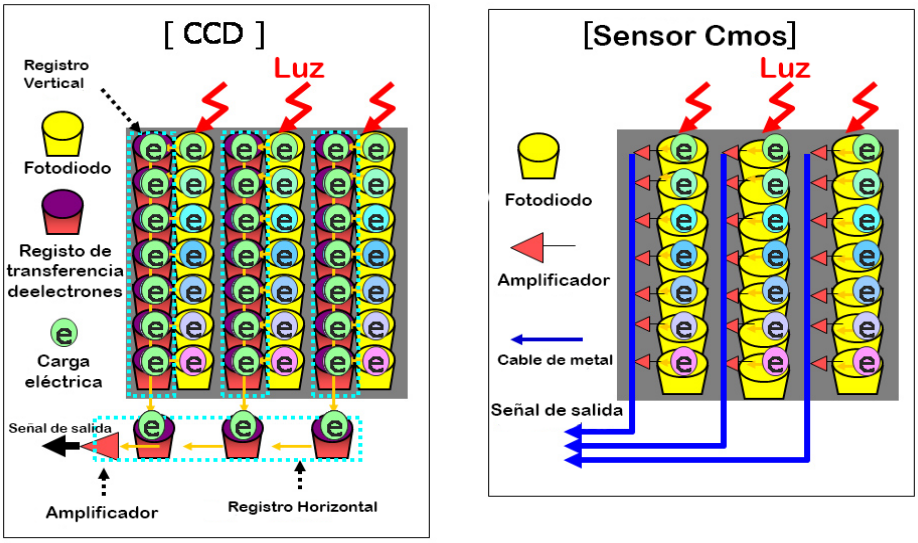


Fig. 2.1: Tipos de sensores

Otro avance en este campo es el mostrado por la compañía Pelican, con su sistema de 16 lentes en un teléfono móvil interconectadas, capaces de crear imágenes muy precisas que permiten hasta generar un modelo 3D con ellas.

Una de las compañías más importantes de sensores de imagen, Sony, acaba de anunciar un par de objetivos independientes a la cámara del móvil, que se conecta a través de la interfaz inalámbrica para enviar las fotos. Se trata de un par de cámaras digitales independientes en formato de objetivos y un sensor en su interior, con ausencia de una pantalla. Se continúan investigando más cambios que logren revolucionar la fotografía móvil digital tal y como la conocemos [3].

2.4. Metadatos Exif

Exif (*Exchangeable Image File Format*). Exif es una especificación para formatos de archivos de imagen usado por las cámaras digitales.). La especificación usa los formatos de archivos existentes como JPEG, TIFF Rev. 6.0.

La estructura general de un archivo JPEG se muestra en la Figura 2.2, los segmentos obligatorios están marcados con gris.

SOI	Start of Image
APP1(no excede 64Kb)	Application Marker Segment 1 (Exif Attribute Information)
APP2 (debe ser almacenado en esta posición si es necesario y puede haber varios)	Application Marker Segment 2 (FlashPix Extension Data)
APPn (no son utilizados por Exif, n valor entre 0 y 15 (incluidos))	Application Marker Segment n
DQT	Define Quantization Table
DHT	Define Huffman Table
DRI	Define Restart Interoperability
SOF	Start of Frame
SOS	Start of Scan
Datos de la imagen	Datos comprimidos de la imagen
EOI	End of Image

Fig. 2.2: Estructura general de un JPG

Los segmentos APPn no son utilizados por Exif, pero la especificación no prohíbe su utilización, por tanto pueden ser utilizados para almacenar para almacenar información de los fabricantes, los cuales deben velar por mantener la compatibilidad con Exif. El orden de los segmentos DQT, DHT, DRI y SOF es intercambiable.

Todos los archivos JPEG empiezan con el valor binario '0xFFD8' (SOI *Start Of Image*) y terminan con el valor binario '0xFFD9' EOI (*End Of Image*). Por tanto un esquema general con los datos Exif actualmente tratado para una imagen JPEG es la Figura 2.3.

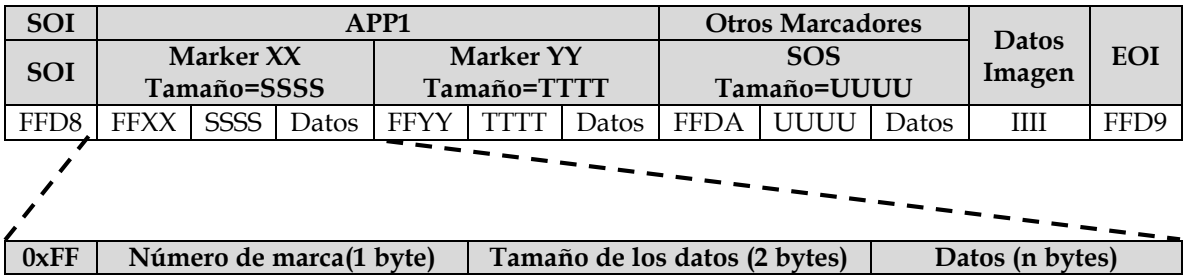


Fig. 2.3: Esquema de metadatos Exif

Toda la información relacionada con Exif está almacenada en el marcador APP1 (*Application Marker 1*), para evitar conflictos con el marcador APP0 del formato JFIF. Por tanto todo archivo Exif comienza con esta estructura.

Los datos APP1 no exceden el tamaño de 64 KB. Los datos de los atributos están almacenados en la estructura TIFF, la cual tiene un máximo de IFDs (el 0th IFD y el 1st IFD). El 0th IFD contiene información sobre la propia imagen y el 1st IFD se utiliza para almacenar todo lo relacionado con la imagen "thumbnail" (imagen en miniatura). Para más información sobre la estructura de los datos de la imagen en miniatura, consultar la especificación.

3. MODIFICACIÓN DE IMÁGENES DIGITALES

Las imágenes tienen un gran poder en el día a día de las personas. La mayor parte de la información que procesa el cerebro es visual. Así, utiliza mayor energía en el procesamiento de imágenes que la información del resto de los sentidos juntos. De hecho, se procesa más rápido una imagen que un texto. Debido a esto, la modificación de imágenes, puede ser realmente peligrosa. Una persona crece pensando que lo que observa es cierto, así, si lo que ve es falso, se crean falsos entendimientos. Esto no es algo nuevo y sucede hoy en día, por ejemplo, las imágenes de las modelos de las revistas están editadas para parecer más delgadas y atractivas a los lectores. Esto provoca que estándares de belleza sean irreales.

Hay una diferencia entre procesamiento y modificación de una imagen. En ocasiones, la modificación de una imagen es insignificante y no conlleva un mayor impacto. Diariamente se hacen modificaciones a una fotografía con el objetivo de corregir pequeñas imperfecciones como ajustes de color, contraste o balance de blancos para hacerla más idónea a lo visto en el momento de su captura para un uso posterior como la publicación de la misma.

De manera rutinaria, se eliminan o minimizan las imperfecciones de una fotografía. Cuando se observa a las personas de un entorno, lo observado se ve influido por factores externos. El foco también se ve afectado por el movimiento de la atención visual. No se aprecian los detalles de la misma manera que se observa el entorno, las caras y las expresiones. Una fotografía es fija y debido a ello no proporciona esas distracciones, por lo que los ojos se fijan en detalles menores como las imperfecciones, las motas de polvo o manchas que de otra manera una persona no es capaz de observar. Una modificación sutil de la imagen puede ayudar a reducir estas distracciones y asemejarla más a su aspecto en el mundo real.

3.1. Objetivo de la Modificación de una Imagen

A menudo, la modificación de una imagen tiene fines artísticos o comerciales. La modificación resulta evidente, es creativa y muy bien hecha. Los artistas que realizan estas modificaciones suelen ser bien conocidos y respetados.

Lamentablemente, en otras ocasiones la modificación de imágenes resulta muy beneficiosa y es realizada con el objetivo de obtener reconocimiento o lucro. Esta práctica está muy extendida en las redes sociales, donde algunas personas obtienen de esta manera millones de seguidores, y así, miles de euros cada mes gracias a la monetización de estas redes. Muchas de estas cuentas comparten imágenes sin acreditación o que han sido falsificadas para llevar a un pensamiento diferente o cambiar la historia. Debido a este problema, han surgido organizaciones y personas que se encargan de exponer este engaño y desacreditar la reputación de estas cuentas para evitar el lucro obtenido con la falsificación de estas imágenes.

3.2. Tipos de Modificación de una Imagen

La modificación de imagenes, está definida como la adición, eliminación y/o cambio de algunas regiones importantes de una imagen sin dejar rastro. Existen varios métodos utilizados para crear o modificar una imagen. Según [4] la modificación digital de imagenes puede ser clasificada como:, modificación mediante copia y pega, división de imagenes y Retoque de imagen.

Adicionalmente, se puede hablar de un tipo de falsificación que está enfocada en la destrucción de la identificación correcta del origen de la imagen, denominada anonimización.

3.2.1. Anonimización de Imágenes

La anonimización de imágenes es la capacidad de evadir las técnicas de identificación de la fuente, que tienen como objetivo obtener información del

dispositivo utilizado para capturar el contenido de una escena. Algunas de estas técnicas han empezado recientemente a utilizarse como evidencia en tribunales. Al mismo tiempo, se cuestiona el respeto que esto tiene sobre los derechos individuales a la intimidad y anonimato. Sobre todo es especialmente importante para fotógrafos, activistas, defensores de los derechos humanos permanecer en el anonimato mientras difunden sus imágenes y vídeos [5].

En [6] se propone disminuir la calidad de la huella PRNU. En la propuesta la imagen se somete a varios procesos de filtrado y a una fuerte compresión con el objeto de que la huella digital PRNU no se pueda extraer de forma fiable. Los resultados de los experimentos realizados muestran que la huella PRNU puede ser identificada realizando una compresión JPEG de la imagen con factor de calidad 50. Incluso después de ocho rondas de reducción de ruido, existe aún una correlación significativa entre el patrón de ruido de la imagen reducida y la huella PRNU del cámara.

En [7] Se propone eliminar de ruido PRNU aplicando *flat-fielding*, durante la producción de la imagen en el sensor de la cámara antes de la interpolación cromática o cualquier otra corrección de color. Esto hace que *flat-fielding* no se puede aplicar a la mayoría de las cámaras.

3.2.2. Copia y Pega de Imágenes

La falsificación mediante copia y pega (o clonación) de imágenes implica operaciones de copiado y pegado de partes de una imagen a otra ubicación en la misma imagen para ocultar un objeto o información importante, o para duplicar ciertos elementos la imagen. Dada que la parte copiada proviene de la misma imagen, no hay un cambio significativo visible en las propiedades de la imagen y textura de la imagen como el color, ruido, y textura, lo que provoca que sea más difícil detectar la modificación [8][9].

Es una de las técnicas de falsificación más utilizadas que emplea técnicas de procesamiento de imágenes típicas. La modificación de una imagen puede modificar la visión que se tiene sobre un hecho actual o cambiar la percepción de la historia. Por ejemplo, Iósif Stalin, el dictador de la Unión Soviética, fue conocido por alterar fotografías para quitar a las personas que se habían convertido en sus enemigos. Como se observa en la Figura 3.1. En ella se muestra a Nikolai Yezhov al lado de Stalin (Figura 3.1.a). Después de que Yezhov cayera en desgracia con Stalin, Yezhov fue eliminado de la fotografía (Figura 3.1.a) y de la historia de Rusia [10].

(a) Foto original (b) Foto modificada

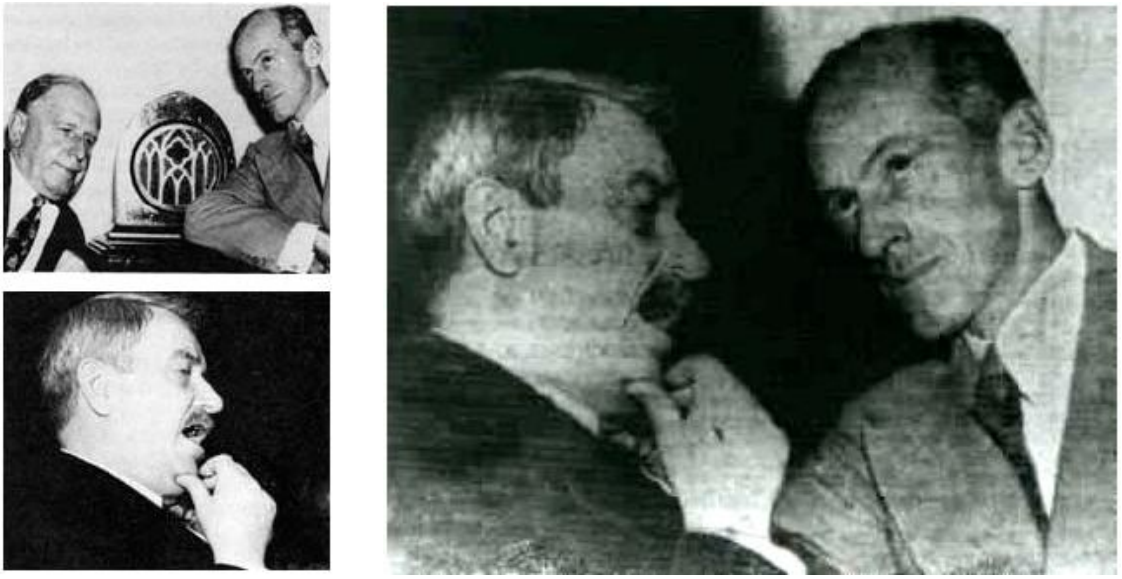
Fig. 3.1. Fotografía de Nikolai Yezhov Iósif Stalin modificada.

3.2.3. Composición de Imágenes

Se conoce como imagen compuesta cuando partes diferentes de una imagen o más imágenes son utilizadas para crear una nueva imagen modificada. La imagen compuesta contiene regiones modificadas y sin modificar y se requiere el uso de operaciones de postprocesado posteriores a la unión.

Para hacer la falsificación imperceptible, algunas de las regiones seleccionadas, tienen que llevar a cabo transformaciones geométricas como rotación, escalado, reducción, recorte, rotación, etc. El paso de interpolación juega una función importante en el proceso de remuestreo y no introduce cambios estadísticos significantes. En remuestreo especifica las correlaciones

periódicas introducidas en los píxeles de la imagen y puede ser utilizado para la detección de la modificación. Un ejemplo, de este tipo de modificaciones es el realizado en una campaña electoral de Estados Unidos (1950). Dos fotografías fueron unidas (Figura 3.2.a), para hacer creer que un senador americano conversaba con el líder del partido comunista americano (Figura 3.2.b). Esta modificación, conllevó probablemente a la derrota del senador debido al pensamiento anticomunista de los Estados Unidos en los años 50 [11].



(a) Fotos originales (b) Foto modificada

Fig. 3.2. Fotografía del senador Millard Tydings modificada.

Actualmente, algunos reporteros gráficos recurren a la falsificación de sus imágenes, como es el caso de Brian Walski, un periodista reconocido y de gran reputación del periódico Los Ángeles Times, que en 2003 publicó una composición de dos fotografías obtenidas en Iraq. En la Figura 3.3 se ve que algunos de los civiles iraquíes que aparecen en el fondo de la imagen están duplicados, proporcionando las pruebas necesarias para indicar que la imagen es el resultado de una composición [12].

(a) Fotos originales (b) Foto modificada

Fig. 3.3. Fotografía modificada por Brian Walski.

3.2.4. Retoque de una Imagen

El retoque de imágenes es el proceso por el cual se realizan pequeñas modificaciones a la imagen para aumentar la definición de la imagen. Este proceso se realiza mediante operaciones de mejora de contraste, reducción de ruido, cambio de color o textura de los objetos, intensificación de las condiciones climáticas, etc. Es comúnmente utilizada en la industria de los medios de comunicación: Está aceptada y es un método recomendable para manipular fotos. No realiza un cambio importante en la imagen y enfatiza (o reduce) alguna deseable (o indeseable) característica de la imagen. Es una técnica popular utilizada en las fotos de las revistas y en películas. La imagen es realzada para hacerla más atractiva y en ocasiones algunas regiones se modifican (para eliminar arrugas) al obtener la imagen final, mientras este tipo de modificación no está valorado como falsificación, se incluye aquí debido a que realiza una modificación efectiva de la imagen original.

Este tipo de manipulación de imágenes digitales se utiliza para fines estéticos y/o comerciales. Sin embargo, también se puede utilizar para cambiar el color de un vehículo implicado en un accidente o para que parezca que un accidente

se llevó a cabo en diferentes condiciones climáticas [13]. Un ejemplo de este tipo de técnicas se muestra en la Figura 3.2.

(a) Imagen original (b) imágenes modificadas

Fig. 3.2. Ejemplo de retoque de una imagen.

4. AUTENTICACIÓN DE IMÁGENES DIGITALES

Teniendo en cuenta los algoritmos avanzados utilizados en la modificación de imagenes, determinar la credibilidad y la integridad de las imágenes digitales se está convirtiendo un reto real para el ojo humano asi como para las máquinas. Por tanto, es muy importante el desarrollo de métodos de detección robustos que identifiquen las operaciones de modificación y validen la autenticidad de las imágenes digitales. Las técnicas actuales de detección de alteraciones en una imagen digital se clasifican en dos tipos: activa y pasiva o ciega [14].

Los métodos de detección activos incrustan una firma digital, una marca de agua digital o metadatos en la imagen original. Esta firma es usada posteriormente para comprobar la veracidad de la imagen. Para ello, es esencial disponer de conocimiento previo de la imagen original y del algoritmo utilizado para codificar la imagen.

Estos métodos tienen grandes limitaciones, entre las cuales se encuentran [4]:

- La marca de agua tiene que ser incrustada por el dispositivo de captura (cámara) o por la persona autorizada que procesa la imagen, lo cual es una aproximación poco práctica debido a la indisponibilidad de realizar las marcas de agua en la mayoría de dispositivos de captura de imagenes.

- La calidad de la imagen, puede ser degradada durante el proceso de la marca de agua.

En los métodos de detección pasivos o ciegos, no se dispone de la imagen fuente. Están basados en el hecho que a pesar de que la modificación es visualmente imperceptible, durante la modificación, las operaciones introducen artefactos nuevos debido al cambio en las propiedades estadísticas fundamentales de una imagen digital. Las incongruencias resultantes de estos

artefactos pueden ser utilizados posteriormente para la detección de la modificación.

4.1. Trabajos Relacionados

En [15] propone un método para detectar si una imagen dada contiene regiones duplicadas apoyándose en el uso de la transformada de Gabor. El método sigue los siguientes pasos:

1. la imagen se convierte a escala de grises y se divide en bloques superpuestos de un tamaño fijo,

2. se extraen características locales de cada bloque utilizando los descriptores HOGM (del inglés *histogram of orientated Gabor magnitude*) que representen el bloque entero.

Finalmente, cada vector de características es lexicográficamente ordenado, y las regiones falsificadas de la imagen son detectadas a través de la identificación de pares de bloques similares. Esta técnica no es eficaz cuando la falsificación incluye post-procesamiento como: pequeñas rotaciones de imagen, escalado, compresión JPEG, difuminado, y ajuste de brillo.

Debido a que la detección de imágenes compuestas no tiene ninguna región de referencia para comprobar regiones duplicadas, en [16] se utiliza la incongruencia en las características de la varianza del ruido restante para detectar regiones modificadas y definir claramente sus contornos. Esta varianza es una clase de patrón de ruido del sensor SPN (del inglés *Sensor Pattern Noise*) resultado de las imperfecciones en la adquisición de una imagen digital y es relativamente estable.

Con este método se obtienen buenos contornos de regiones modificadas. Más detalladamente, los componentes de la imagen se extraen para realizar una detección adaptativa. Luego, se calcula la varianza del ruido que queda después

de reducir el ruido en cada componente de la imagen. Finalmente, las regiones modificadas son detectadas utilizando la varianza del ruido restante de los componentes. Los resultados de los experimentos realizados muestran que el método propuesto tiene una buena tasa de detección de imágenes compuestas.

Cuando una imagen es falsificada por la combinación de varias imágenes es necesario realizar modificaciones como por ejemplo, cambiar el tamaño de las regiones de las imágenes que serán combinadas, con el objetivo de que la falsificación sea convincente. Sin embargo, aunque no es posible detectar las modificaciones visualmente, a través de las correlaciones introducidas en la imagen al modificarlas se puede detectar la falsificación.

En [17] se presenta una técnica de detección de falsificaciones que utiliza el algoritmo de Expectación / Maximización (EM). La propuesta se basa en las correlaciones introducidas por el re-muestreo, donde se supone que cada muestra pertenece a una de las siguientes opciones: a) Muestras que estén correlacionadas con sus vecinos; y b) Muestras que no tienen correlación con sus vecinos.

En [18], se propone un método de detección de falsificaciones en una imagen digital usando DyWT, una variación de la transformada wavelet. El sistema completo se conoce como DyWT (*Undecimated Dyadic Wavelet Transform*), similar a DWT (*Discrete Wavelet Transform*), pero sin presentar algunas carencias como: DWT no es invariante respecto a traslaciones causando una excesiva cantidad de coeficientes que dificultan la estimación de ruido. El uso de la transformada wavelet se prefiere sobre la transformada de Fourier en cuanto a procesamiento de imágenes, pues no sólo extrae información de escalado, sino también información de localización. La transformada wavelet descompone una imagen en su representación media y en distintas representaciones de detalles direccionales.

Para el reconocimiento de patrones en la imagen, es preciso que la técnica sea

inmune a rotaciones, pues a veces se copian elementos rotados. Si hay elementos parecidos en una imagen, tratar sólo con la subbanda LL1 los identifica como objetos copiados (falsos positivos). La subbanda HH1 los distinguiría por el nivel de ruido de cada uno. Por lo tanto, ambos elementos deben usarse a la vez. También es necesario convertir las imágenes a escalas de grises antes de usar el método propuesto. La aplicación del método es bastante complejo y tiene la dificultad de que al formar bloques en la imagen no se sabe si hay rotaciones, por ejemplo. Aun así, es un sistema que produce unos resultados cercanos al 100%.

5. THEIA: HERRAMIENTA PARA EL ANÁLISIS FORENSE DE IMÁGENES Y VÍDEOS DIGITALES

En este capítulo se presenta Theia, una herramienta para el análisis forense de imágenes y vídeos digitales que facilita la extracción y el tratamiento de metadatos Exif en imágenes JPEG y átomos en vídeos MP4. A grandes rasgos la herramienta se divide en dos grandes partes: Tratamiento individual y tratamiento masivo de imágenes y vídeos.

5.1. Tratamiento a Nivel Individual

Permite obtener la información Exif detallada de una imagen individual, situar la imagen en Google Maps y Google Earth (si posee información de geoposicionamiento). La estructura general se puede observar en la Figura 5.1.

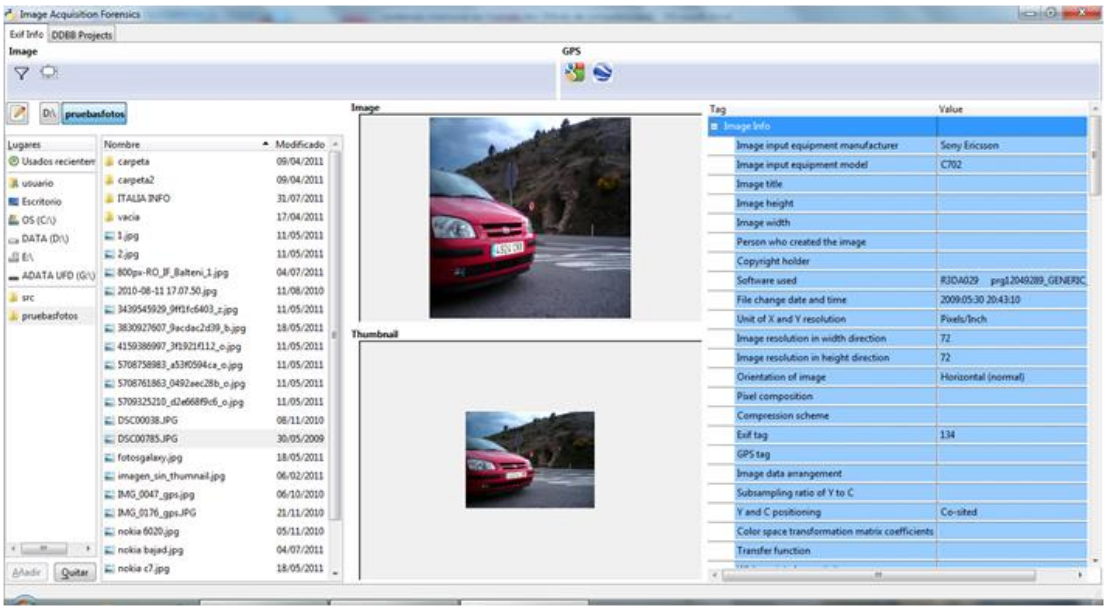


Figura 5.1. Apariencia general de la pestaña *Exif Info*

Como estructura general se puede apreciar a la izquierda de la imagen un navegador de archivos, en el centro la imagen del archivo seleccionado y su correspondiente thumbnail (es el incluido en el propia archivo de la imagen no ninguna generación propia del programa) y a la derecha las etiquetas Exif con

su correspondiente información. De esta estructura cabe destacar en la interfaz gráfica que es totalmente configurable a nivel de tamaños, es decir todos los separadores entre las distintas zonas se pueden mover.

La información Exif se ha organizado en 6 grupos: *Image*, *Exif*, *GPS*, *Interoperability*, *Thumbnail* y *Maker Note*.

- ***Image Info***: En este bloque se almacenan las etiquetas con información relativa a la propia imagen y que no tienen relación directa con el entorno y el momento de la captura. Por ejemplo la marca y modelo de la cámara, el tamaño de la imagen, la unidad utilizada en la resolución X e Y, etc.

- ***Exif Info*****:** En este bloque se guardan las etiquetas con información relativa al momento o al entorno de la toma de la imagen. Dentro de este bloque se encuentra por ejemplo la información referente al flash, hora de toma y generación de la imagen, configuración de la lente, etc.

- ***GPS Info***: En este bloque está toda la información relativa al geoposicionamiento. Por ejemplo información de latitud, longitud, altitud, el estado del receptor GPS, etc.

- ***InterOperability Info***: En este bloque se incluyen las etiquetas relativas a la información de las reglas de interoperabilidad, como pueden ser *Exif R98*, *DCF thumbnail file* o *DCF Option file*.

- ***Thumbnail Info***: En este bloque se encuentran todas las etiquetas relativas a la información de *thumbnail*. Por ejemplo su tamaño en vertical y horizontal y el esquema de compresión utilizado.

- ***Maker Note Info*****:** Es una etiqueta individual que almacena la información que cada fabricante puede insertar de forma opcional y que no ha sido recogida en ninguna etiqueta Exif.

El formato de esta información es libre y no tiene una estructura prefijada, cada fabricante utiliza la suya propia que incluso puede ser diferente para distintos modelos de la misma marca. Por tanto se muestra como una secuencia de bytes (en hexadecimal). Si se conoce la estructura estos bytes pueden ser decodificados de forma manual.

Asimismo, se pueden extraer los datos de geoposicionamiento que estén incluidos en las imágenes. Si la imagen no tiene la suficiente información para poder ser mostrada en alguna de las opciones al pulsar la opción de geoposicionamiento se mostrará un mensaje indicándolo (*Not enought GPS information*). El geoposicionamiento se puede realizar desde dos opciones: posicionamiento en Google Maps y en Google Earth. En la primera se abrirá el navegador web por defecto del sistema operativo y se mostrará la ubicación inserta en los metadatos de la imagen en un mapa de Google Maps (es necesario conexión a internet). La Figura 5.2 muestra un ejemplo de geoposicionamiento en una fotografía en Google Maps.

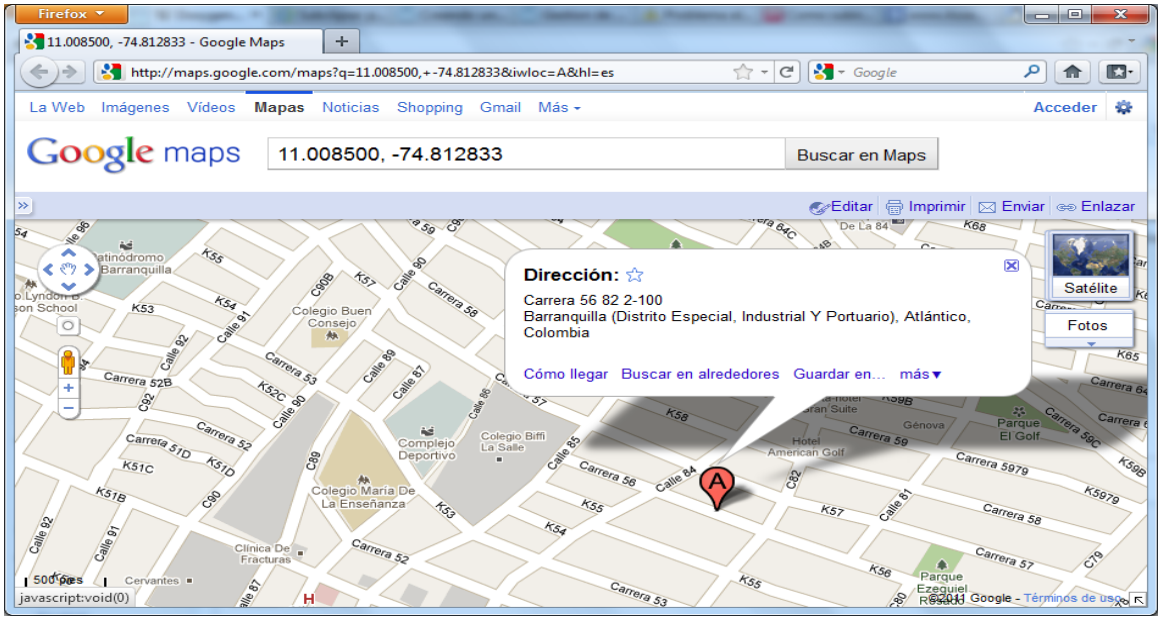


Figura 5.2. Geoposicionamiento en Google Maps

En la segunda opción se abrirá un menú para poder almacenar un archivo de extensión “kml”. Este archivo podrá ser posteriormente abierto si está instalada la aplicación Google Earth, en la cual se mostrará igualmente la posición geográfica almacenada en los metadatos de la imagen (es necesario conexión a internet).

5.2. Tratamiento a nivel de grupo

Permite hacer análisis de imágenes en grupo. Cada grupo es totalmente independiente entre sí. Su apariencia gráfica general puede verse en la Figura 5.3.

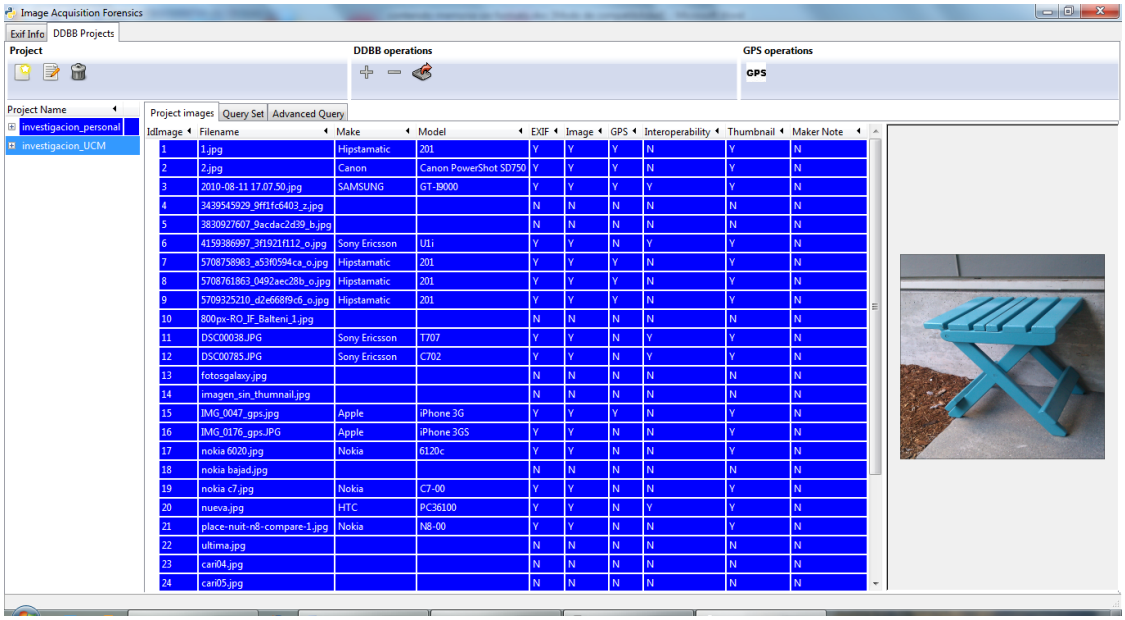


Figura 5.3. Apariencia general de la pestaña *DDBB Projects*

Lo primero a destacar en esta funcionalidad es que las imágenes se tratan en grupos llamados proyectos. Estos grupos pueden ser de una o más imágenes. Cada proyecto es totalmente independiente entre sí. Se busca acercar la realidad del día a día del analista forense a la herramienta, es decir, el analista tendrá diversos casos de análisis disjuntos los cuales podrá tratar en proyectos distintos.

En la parte central de la pestaña *DDBB Projects* y dentro de ésta en la pestaña *Project Images* se muestran una lista de las imágenes del proyecto seleccionado en la lista de proyectos.

Para cada imagen se muestra su identificador interno de la base de datos (para permitir el caso de archivos con el mismo nombre), el nombre del archivo, la marca y el modelo de dispositivo que la creó (si existe). Además se presenta la información de si posee metadatos en los distintos grupos Exif que analiza la herramienta. Asimismo se visualiza el contenido de cada una de las imágenes a la derecha según se van seleccionando. Un ejemplo de captura de esta funcionalidad se muestra en la Figura 5.4.

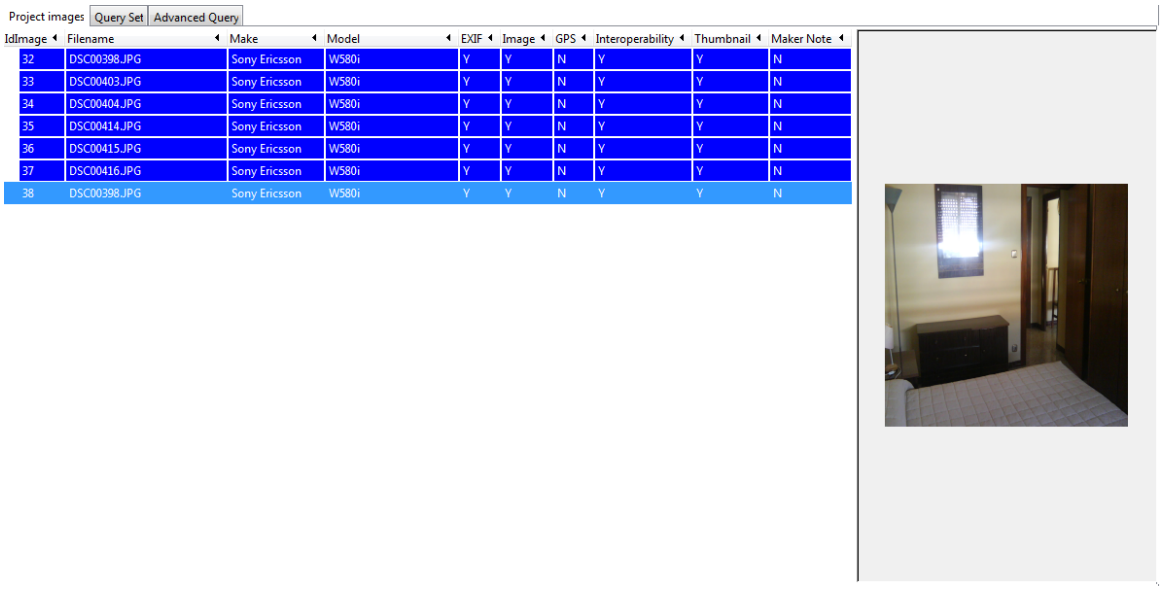


Figura 5.4. Visualización de las imágenes de un proyecto

Los diferentes análisis que se pueden realizar sobre cada proyecto son los siguientes: administración de imágenes (añadir y eliminar imágenes), consultas preestablecidas, consultas avanzadas y geoposicionamiento de las imágenes.

- *Consultas preestablecidas*: Permite crear consultas agregando etiquetas Exif (y otras adicionales que añade la aplicación que ayudan al análisis forense) sobre las imágenes del grupo seleccionado. La consulta agrupa las imágenes por los criterios seleccionados y muestra el número de imágenes que hay en

cada uno de los grupos formados, como puede verse en un ejemplo en la Figura 5.5. En las consultas permiten escoger 5 campos de agregación como máximo (por defecto se realiza sobre *Make* y *Model*, aunque ser pueden elegir cualesquiera). Para escoger los distintos campos hay que pulsar sobre el botón *Query Set*

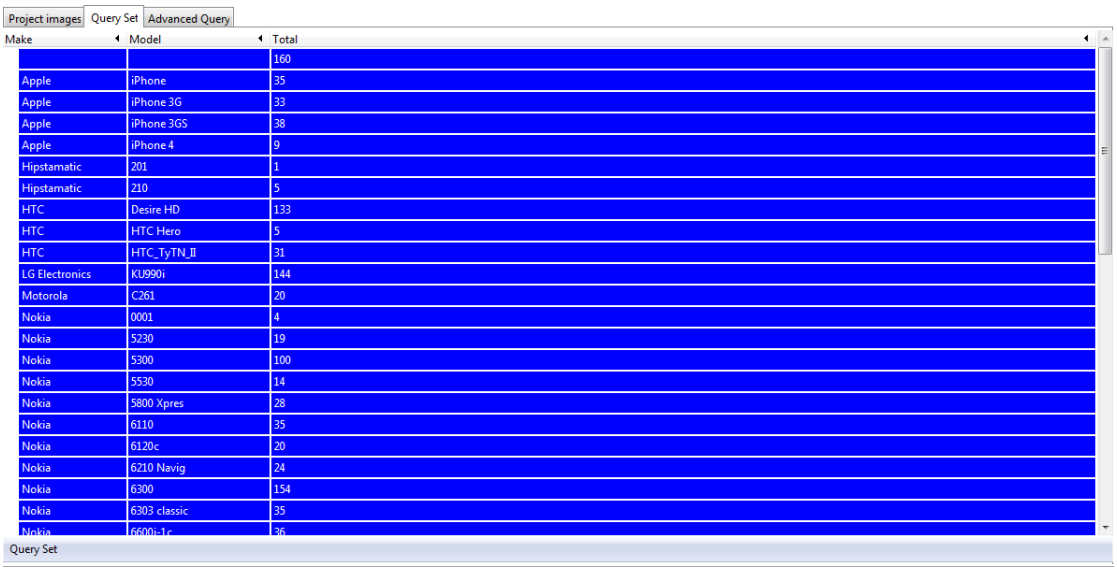


Figura 5.5. Query Set

- *Consultas avanzadas*: Permite la creación de consultas sobre imágenes de un grupo configurando los datos Exif a mostrar y los filtros a aplicar. Es decir, muestra la información de las imágenes de los campos seleccionados que coincidan con uno de los valores de cada uno de los filtros configurados. Asimismo, se permite el almacenamiento permanente de consultas. Una visión general se muestra en la Figura 5.6.

  En *Advanced Query* hay que distinguir dos grandes bloques: la configuración de la consulta y su almacenamiento. Con respecto a la configuración de la consulta avanzada hay que tener en cuenta la configuración de las columnas de los resultados y la configuración de los filtros. En esta consulta se muestran los valores de los campos seleccionados por la configuración de las columnas de los resultados que cumplen las restricciones indicadas en la configuración de los filtros.

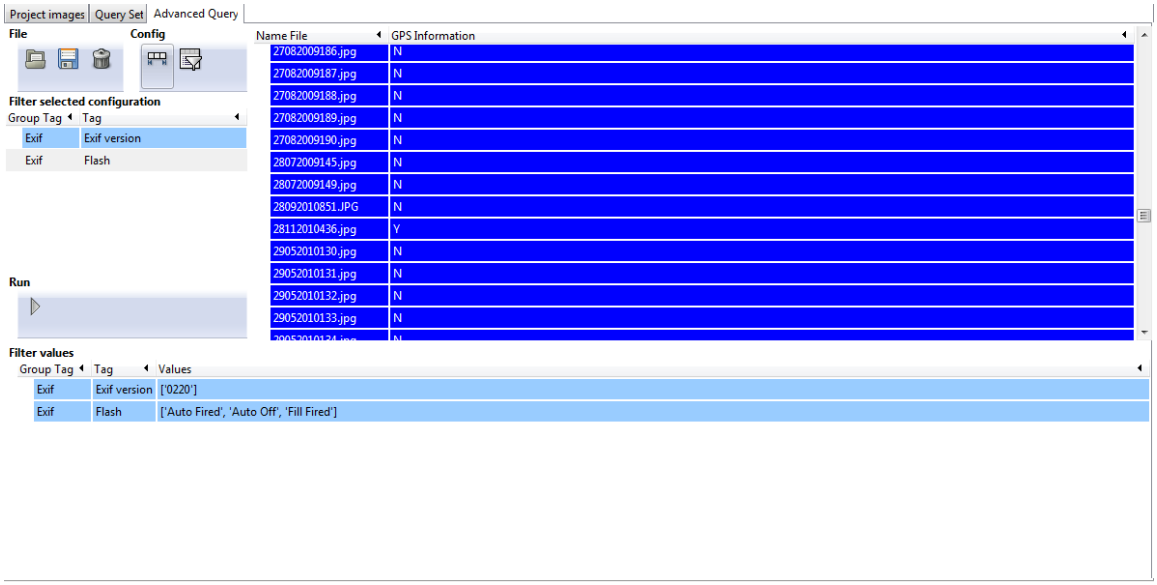
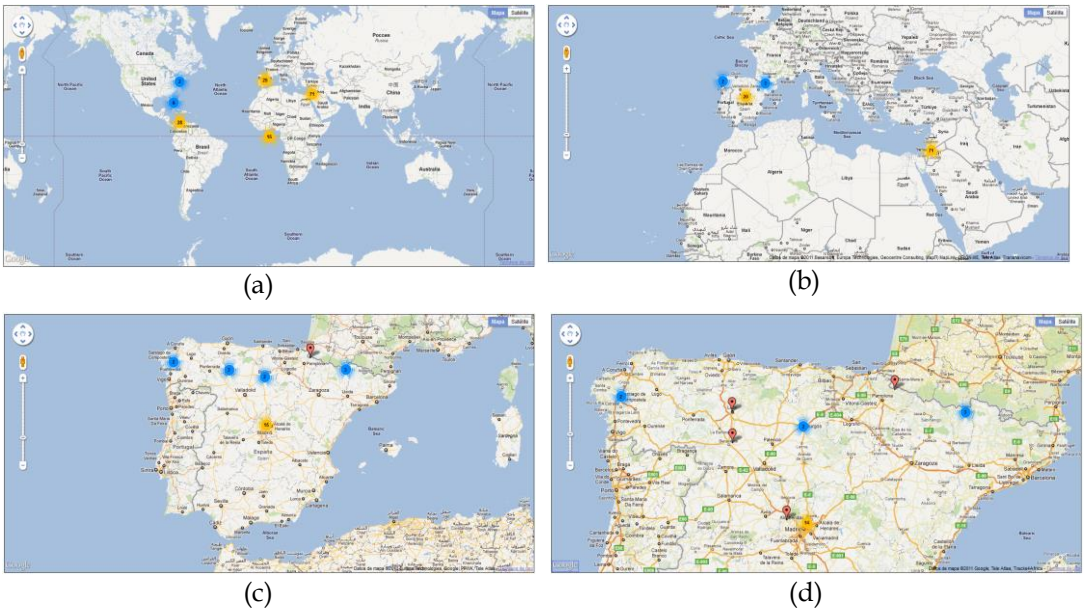


Figura 5.6. *Advanced Query*

- *Geoposicionamiento*: Análogamente al tratamiento de imágenes a nivel individual, existe una funcionalidad que permite el tratamiento de la información de geoposicionamiento para un grupo de imágenes. Esta opción permite la selección de algunas o de todas las imágenes de un grupo con información de geoposicionamiento para la creación de un mapa en Google Maps que sitúe a las mismas. En el mapa se agrupan las imágenes por zona y, a medida que se aumenta el *zoom*, se van detallando las coordenadas. La Figura 4.7 muestra un ejemplo del mapa generado y el proceso de aumento del *zoom* en una zona concreta (desde la Figura 4.7 (a) hasta la Figura 4.7 (d)).



(a) (b)

(c) (d)

Figura 5.7. Geoposicionamiento de un grupo de imágenes en Google Maps

6. CONTRIBUCIÓN

Uno de los principales problemas en el mundo digital, es la gran cantidad de información que se obtiene cada día. Por ello, es necesario contar con herramientas que ayuden a filtrarla y procesarla. En este trabajo se tiene como objetivo desarrollar un método que proporcione de una manera sencilla la capacidad de diferenciar una imagen sin ninguna alteración posterior a su captura que afecte a la integridad de dicha imagen, de aquellas que si han sufrido modificaciones. La importancia de poder determinar la veracidad de las imágenes ha ido en aumento, siendo cada vez más importante disponer de herramientas y medios que ayuden y faciliten dicha tarea. Con este objetivo, en este trabajo se ha implementado una herramienta que realice un estudio de imágenes digitales para verificar la autenticidad de esta información. Por razones de confidencialidad del proyecto se ha omitido información del trabajo desarrollado para no infringir la normativa correspondiente.

6.1. Consideraciones Generales

Los principales hándicaps de la verificación de imágenes son el tiempo y los recursos de cálculo necesarios para realizar la verificación. La cantidad de información (imágenes) a procesar, la gran diversidad de dispositivos, cada uno con una gran cantidad de características diferentes, dificultan encontrar un método general que permita dicha verificación. Además, la falta de un estándar en el mundo digital, donde cada fabricante decide lanzar sus modelos con características únicas. Por ejemplo, desde el sensor utilizado por la cámara (CCD, Super CCD, CMOS, CCD RGBE, Foveon X3, etc.), hasta el modelo de color utilizado (RGB, CMYK, HSL, sRGB, RYB, etc.) hacen que un método de verificación válido para una determinada marca y modelo no lo sea para otro de otro fabricante o en ocasiones hasta modelos del mismo fabricante.

Tras un extenso análisis de las características de las imágenes digitales para diseñar un método que permita de manera poco costosa (en términos de recursos y tiempo), se optó por el uso de las Tablas de Cuantificación, una característica que se encuentra en todas las imágenes digitales que proporciona una marca única de un determinado dispositivo y/o software.

Su extracción se puede realizar desde la propia imagen sin necesidad de apoyo de datos adicionales sobre su obtención. Además los métodos "anti-forenses" que buscan dificultar la tarea de verificación de imágenes. Se centran en otros aspectos y no realizan cambios en las tablas de cuantificación, o si lo hacen estas herramientas dejan una huella en dichas tablas que permiten comprobar y marcar que ha sufrido una manipulación.

6.2. Diseño

Como aspectos relevantes de la implementación pueden señalarse las diversas herramientas utilizadas para desarrollar los distintos elementos:

- El lenguaje de programación utilizado para la codificación de la aplicación es Python 2.7 bajo el sistema operativo Linux con Distribución Debian Jesie 8. De éste se destaca la utilización de la librería PIL que facilita diversos tipos de tratamientos sobre imágenes. Se extendió la implementación de los siguientes paquetes:
    - **Exif**: Contiene las clases y estructuras de datos auxiliares que obtiene los metadatos Exif hasta la versión 2.3. Se modificó el algoritmo de extracción de metadatos Exif para incluir la extracción de las tablas de cuantificación.
    - **BBDD**: Contiene las clases para el control de la base de datos que permiten la conexión y la gestión de todos los datos.

- **Exception**: Contiene las clases para el control de excepciones de manera más adecuada.

- Se ha utilizado como plataforma de programación Eclipse Neon que permite crear entornos integrados de desarrollo multilenguaje y adaptables. Ofrece una extensa flexibilidad de configuración con los complementos necesarios para adaptar los requerimientos de desarrollo que no estén contemplados dentro de las configuraciones básicas. Para este caso concreto se requirió el uso del complemento Pydev de Eclipse para permitir el desarrollo en Python.

- Para la realización de la documentación interna del proyecto se ha utilizado Doxygen.

- El motor de base de datos utilizado es MySQL. En ella se almacena toda la información necesaria para el funcionamiento del algoritmo. En ella almacenará las estructuras para analizar las tablas de cuantificación.

6.3. Funcionamiento

El proceso de autenticación de imágenes de dispositivos móviles se realiza en 2 fases:

6.3.1. Fase de Entrenamiento

En esta fase se obtienen las tablas de cuantificación de referencia tanto de los diferentes programas de manipulación de imágenes como de las tablas de cuantificación de cada Marca y modelo.

Adicionalmente, se extrae toda la información de los metadatos Exif para analizar las etiquetas almacenadas y los errores a la hora de almacenarlos y que crean una especie de huella en la imagen. La extracción de las tablas de cuantificación de referencia y los metadatos extraídos se almacenan durante

esta fase, para posteriormente evaluar las imágenes objeto de investigación.

Posteriormente, se analizan las etiquetas extraidas y la tabla de cuantificación para crear un patrón de referencia del modelo de un fabricante procesado por una herramienta de edición de imágenes. Esto es posible ya que las herramientas, almacenan información en los metadatos Exif a la hora de procesar la imagen.

6.3.2. Fase de Autenticación

En esta fase se decide si una imagen analizada tiene indicios de haber sufrido algún tipo de modificación.

En esta fase se procesan las imágenes investigadas de forma individual. A la hora de analizarlas para detectar su manipulación, la herramienta dispone de la información con el patrón de referencia. Cada imagen es procesada realizando un análisis de la estructura del archivo utilizando los metadatos Exif almacenados en el archivo de la imagen. Se extraen las etiquetas establecidas en la fase de entrenamiento para analizarlas con el patrón de referencia tanto de la imagen como de la imagen resumen. Asimismo, de la información Exif se extraen los datos referentes al *thumbnail* de la imagen digital ya que contiene la imagen resumen original de la imagen. Posteriormente, se genera una imagen resumen a partir del contenido de la imagen.

Una vez extraídos, se evalúan estos datos con los datos de referencia almacenados. Se comprueba primero si han sido manipuladas mediante una herramienta de edición, si no está, se comprueba si se tiene la información para esa marca y modelo. Si estos datos no coinciden es porque la fotografía a pasado por una herramienta externa a la del dispositivo móvil. Y se procesde a realizar el análisis de la imagen resumen almacenada en los metadatos Exif. Se genera una imagen resumen estimada a partir del contenido de la imagen. Para generar el thumbnail se debe tener en cuenta toda la información almacenada en el "IFD Thumbnail" de los metadatos Exif para estimarlo lo más parecido

posible al thumbnail almacenado en los metadatos Exif.

A continuación, se realizan operaciones de correlación en ambas imágenes resumen (el almacenado en los metadatos Exif y el generado a partir del contenido de la imagen) y se comparan para detectar si la imagen ha sido manitpulada

6.4. Evaluación

Para el estudio de la capacidad de detección de las técnicas empleadas en este trabajo para detectar la manipulación se ha realizado un estudio de 10 imágenes de las marcas y modelos indicados en la Tabla 6.1.

Para ello, se han ejecutado tres pruebas diferentes, estas pruebas tienen las siguientes características:

1. Se ha realizado una modificación en dichas imágenes antes de su análisis. Esta modificación consiste en lo siguiente: Cambio en los valores de brillo/contraste.

2. Se ha realizado una modificación en dichas imágenes antes de su análisis. Esta modificación consiste en lo siguiente: Copiado y pegado de parte de la imagen en sí misma

3. Se ha realizado una modificación en dichas imágenes antes de su análisis. Esta modificación consiste en lo siguiente: Recorte de la imagen.

4. Imágenes con modificaciones externas: cambios en los datos EXIF de Exposición y Geolocalización.

Los resultados de estos experimentos se observan en la Tabla 6.1.

Marca	Modelo	Tasa de detección		
		Experimento 1	Experimento 2	Experimento 3
Apple	4S	100%	100%	100%
	5	100%	100%	100%
	5S	100%	100%	100%
	6	100%	100%	100%
Blackberry	8520	100%	100%	100%
BQ	Aquaris E4.5	100%	100%	100%
	Aquaris 5	100%	100%	100%
Huawei	Y635-L01	70%	70%	70%
	U8815	60%	60%	60%
LG	E400	100%	100%	100%
	Nexus 5	100%	100%	100%
	P760	100%	100%	100%
Motorola	Moto G 1ª Generación	100%	100%	100%
	Moto G 2ª Generación	100%	100%	100%
Nokia	Lumia 800	100%	100%	100%
One Plus	One Plus One	100%	100%	100%
Samsung	Galaxy Nexus	100%	100%	100%
	Galaxy S3	50%	50%	50%
	Galaxy S4 Mini	100%	100%	100%
	Galaxy S5	100%	100%	100%
	Galaxy S6	100%	100%	100%
	GT-i9001	60%	60%	60%
	GT-i9100	100%	100%	100%
	GT-s5830	100%	100%	100%
	GT-s5830m	100%	100%	100%
	Galaxy S3 Neo	100%	100%	100%
Sony	C2105	80%	80%	80%
	ST25a	100%	100%	100%
	ST25i	100%	100%	100%
	Xperia M2	100%	100%	100%
Xiaomi	MI3	60 %	60 %	60 %
Zopo	ZP980	100%	100%	100%

Tabla 6.1. Resultados del experimento.

Como se puede observar los tres primeros experimentos, los mismos resultados son similares, esto se debe a que la tabla de cuantificación no se ve afectada por la modificación que se aplique a la imagen sino al programa empleado para la modificación y las características de la foto original. Las marcas y modelos con una tasa de detección menor han sido afectadas por cambios en la versión de manipulación de las imágenes que provocan pequeñas variaciones en las tablas de cuantificación, que conllevan a que falle su detección

7. CONCLUSIONES Y TRABAJO FUTURO

7.1. Conclusiones

Una vez obtenidos los resultados se obtienen las siguientes conclusiones. Como se puede observar en las tablas, la tasa de detección es muy alta, dando casi el 100% en algunas marcas y modelos. Sin embargo para determinadas marcas hay variaciones en las tablas de cuantificación lo que provoca que la detección de la manipulación falle. Esta variación dentro de un mismo modelo se debe a la realización de cambios en las opciones de configuración de algunas características para la obtención de la imagen. Además, esta alta tasa se ha obtenido gracias al entrenamiento previo de la aplicación con las imágenes de las marcas y modelos seleccionados, sin dicho entrenamiento, no es posible determinar correctamente la veracidad de las imágenes.

Por ello, a la hora de verificar una imagen que una vez estudiada no se encuentra en la base de datos del programa, el programa fallará y requerirá obtener unas cuantas imágenes del dispositivo con el que se obtuvieron, lo cual no siempre es sencillo ya que si no se dispone del dispositivo, o los parámetros EXIF que identifican al dispositivo son manipulados supone un gran hándicap y puede provocar un fallo a la hora de detectar la manipulación. Pero es un método con un bajo coste que acompañado junto al otro método complementario, el cálculo de RMS, garantiza una mayores tasas de acierto y menor número de falsos positivos.

Una vez finalizado el estudio de los resultados, es el momento de realizar una evaluación general. Se cree que este trabajo ha cumplido con los objetivos marcados al principio del proyecto. Se ha explicado cómo ha evolucionado el mundo del análisis forense digital de imágenes así como las herramientas anti-forenses que dificultan el trabajo de verificación de imágenes. Se ha demostrado como aplicar una técnica que permite realizar una análisis de la autenticidad de

las imágenes que no requiera una gran cantidad de recursos y tiempo para realizar un análisis rápido y que proporcione resultados inmediatos para que el analista obtenga las evidencias necesarias para poder dictar un veredicto.

Como conclusión creo que el trabajo realizado ha demostrado las técnicas necesarias y los posibles caminos que se pueden tomar para convertir la herramienta en un referente para el análisis forense y además de proporcionar un punto de partida para futuras adiciones que mejoren la herramienta para su uso en entornos profesionales y su posible aplicación en campos de trabajo como el policial o judicial.

7.2. Trabajo Futuro

Como trabajos futuros posibles pueden señalarse los siguientes:

- Creación de una gran base de datos: Una base de datos con información sobre las tablas de cuantificación de multitud de fabricantes, modelos y software de edición fotográfica, proporcionada por los propios fabricantes y desarrolladores ayudaría a mejorar las tasas de detección y a la vez eliminar posibles falsos positivos.

- Estudio de los patrones: El estudio de todos los patrones que componen el proceso de obtención de una imagen digital, desde su obtención en el sensor de imagen, al procesado y post-procesado de la fotografía podría revelar huellas únicas que puedan establecer un método general que diera lugar a un método de verificación más rápido o más eficaz.

- Desarrollo de frameworks y bibliotecas de manipulación de imágenes: Uno de los problemas para el estudio de las imágenes digitales es el soporte que ofrecen los principales lenguajes de programación y frameworks de desarrollo. No todos disponen de las herramientas necesarias para obtener la información que se desea extraer de las

imágenes y cuando se trata de obtener información a un nivel de abstracción mayor se hace casi imposible encontrar una herramienta que nos permita hacer determinados procesamientos digitales.

RESUMEN EN INGLÉS

8. INTRODUCTION

8.1. Motivation

The popularization of cameras on mobile phones has caused a revolution in the world of photography. This has a lot of advantages but also several drawbacks. Mobile phones have made available to lovers of photography, an accessible way for beginners in this world, however, this has led to an incredible increase in the number of digital content and quality of these. In the environment in which we live, there are too much information, which allows to be the more informed generation but we do not have the necessary mechanisms to process and filter out unwanted elements. Because of this we have lost our capacity of critical thinking, accepting any information obtained as true without questioning their origin.

The camera technology of mobile phones continues improving and increasing its performance, although compact or SLR camera will maintain its use in the professional segments. Mobile cameras have put in serious trouble to the compact cameras, but have not yet managed to displace DSLR (Digital Single Lens Reflex) or a good CSC (Compact System Camera). Mobile photography has several advantages over traditional cameras, especially the instantaneity of the photographs, because one not always have a DSLR camera, but always has the mobile phone, in addition, compact cameras fit better when you want to photograph items with a higher quality or better features. Both technologies can coexist and their difference is based on the characteristics that are desired when making the photography. The important thing is to capture the moment, no matter the medium [1].

Improvements in the technology segment of mobile phones: better cameras, newer screens, Internet access ... has caused a change in the way of working for many professionals. Thanks to the Internet and the improvements of these

technologies have turned these devices into real multimedia, entertainment and communication centers. In the scope of Journalism, it has democratized and improved dissemination. Thanks to the mobile devices, communicators have gone through a series of changes such as the possibility of obtaining images captured by the users themselves, for example, protests in the Arab spring, and the standardization of the orchestra journalism, where the editor should be being able to write the news and also take part on other elements such as the inclusion of their own images and videos [1].

However, doubts about the validity that may have WhatsApp messages, photos, SMS and other content present in a Smartphone, Tablet, among other mobile devices. The answer is variable and requires an analysis of each case. What I can say is that the content is perfectly valid as evidence in court proceedings, providing that, at the time of obtaining such evidence fundamental rights are respected. Once said this, it is necessary to analyze to what extent such evidence is sufficient, especially in criminal proceedings to prove the innocence or guilt of a criminal defendant supported by the presumption of innocence.

For an evidence to be considered and lead to a conviction penalty it must fulfill a number of properties. First, the origin of the test is essential, e.g., It will only have validity, that evidence obtained by order of a judge and it is provided by the company itself that "stores" data (Twitter, Facebook, etc.). However, if the evidence is provided by the complainant itself, it is necessary to provide a list of requirements to check their veracity. This is due to the ease with which such evidence can be modified, such as deleting some unwanted image element, it is also possible, that someone else has intercepted communication or mobile device to impersonate the user or simply these evidences could have been modified by a computer technician.

According STS 1415/2003, of October 29, the right to the presumption of innocence of art. 24.2 EC requires the trial court the following:

- That there is a test containing charge.
- That such incriminating evidence has been obtained and provided to the process in accordance with the provisions of the Constitution and Procedure Act.
- That the incriminating evidence is reasonably considered sufficient to justify the criminal conviction.

Therefore, any means of "technological test" can be used in court proceedings. However, it may not be enough to convict a defendant. So, using any evidence available is as important as demonstrating that such evidence, have enough validity to get a criminal conviction. To achieve this, it is essential that such evidence has been obtained through the appropriate judicial authority or to be supported by a computer expert. Hence the nowadays importance of forensic analysis of digital images of mobile devices. In [2] a study on the need for specific forensic analysis techniques for mobile devices is presented.

8.2. Objectives

This Final Degree Work (TFG) has the following objectives:

- Conduct a study of the related work about the types of possible changes in images to make a classification of the most important.
- Conduct a study of the techniques of forensic authentication of existing digital images in the literature in order to analyze and understand the most relevant techniques.
- Implement an algorithm to determine whether a digital image has been

manipulated using the thumbnail image stored in the Exif metadata.

8.3. Work Schedule

The project has been developed in 3 phases: Definition, Execution and Documentation Project. Activities in these phases are presented in Table 8.1.

During the first phase the objectives and scope of the Final Degree Work were established, meetings with the team of tutors and monitoring the work done during the preparation of work. Later, during the implementation phase, the project defined in the previous stage was developed. This phase consists of the following steps: requirements specification, design, implementation and testing. During the completion of this phase, they were conducted monitoring and control project progress to track and monitor the realized activities.

Finally, in the documentation phase, all the necessary tools for necessary the preparation of the Final Degree Work documentation was performed. This phase was carried out in conjunction with the two previous phases.

Name of the task	Duration (days)	Start	End
• **Project definition**	**40**	**23/11/15**	**29/01/16**
- Weekly control meeting with the tutors.			
- Study of the types of image manipulations			
- Study of the techniques of authentication images obtained by mobile devices			
- Project definition			
• **Project execution**	**130**	**01/02/16**	**01/07/16**
- Requirements specification			
- Design			
- Implementation			
- Tests			
- Control			
• **Documentation**	**150**	**14/12/15**	**29/07/16**
- Project documentation generation			
- Memory preparation			

Table 8.1. Phases of the project

9. CONCLUSIONS AND FUTURE WORK

9.1. Conclusions

The conclusions obtained from this work are as follows:

After obtaining the previous results, the following conclusions were obtained. As can be seen in the tables, the detection rate is very high, giving almost 100% in some brands and models. However, for certain brands there are variations in quantization tables making image manipulation detection to fail. This variation within a same model is due to the changes made in the settings of some features for obtaining the image. In addition, this high rate has been obtained thanks to previous training application with images of selected brands and models, without such training, it is not possible to correctly determine the veracity of the images. Therefore, when verifying an image that once it has been studied and is not in the database, the program will fail and will require to get a few pictures of the device which they were obtained with, which is not always easy because if the device is not available, or the EXIF parameters that identifies the device are manipulated this is a great handicap and can cause a failure while detecting the tampering. But this is a method with a low cost, along with the other complementary method, the RMS calculation, it ensures a greater success rates and fewer false positives.

Once the study of the results is made, it is time to make an overall assessment. It is believed that this work has met the objectives set at the beginning of the project. It was explained how the world of digital image forensics has evolved, as well as, the counter-forensic tools that makes more difficult the work of image verification. It has been shown how to apply a technique that allows an analysis of the authenticity of the images that does not require a lot of resources and time to make a quick analysis and provide immediate results to the analyst by obtaining the necessary evidence to provide

a verdict.

In conclusion I believe that the work done has shown the necessary techniques and the possible paths that can be taken to make the tool a reference for the forensic analysis and it also provides a starting point for future additions to improve the tool for using it in professional environments and their possible application in fields like the police or judiciary.

9.2. Future work

Possible future work can be identified as coming next.

- Creating a big database: A database with information about the quantization tables of all the possible manufacturers, models and photo editing software, provided by the own manufacturers and developers to help improve detection rates while eliminating possible false positives.

- Study of patterns: The study of all patterns that make the process of obtaining a digital image, from obtaining the image in the sensor, the processing and post-processing of the photography could reveal unique traces that can establish a standard method giving place to a method with a faster or more effective verification.

- Development of frameworks and libraries of image manipulation: One of the problems in the study of digital images is the support offered by the major programming languages and development frameworks. Not all have the necessary tools to get the information necessary to be extracted from the images and when it comes to getting information to a higher level of abstraction is almost impossible to find a tool that allows us to do some digital processing.

REFERENCIAS

[1] J. Bañuelos, and F. Mata. "Fotografía y dispositivos móviles". Escenarios de un Nuevo Paradigma Visual. México, Tecnológico de Monterrey, Porrúa Print, 2014

[2] V. L. L. Thing, K. Y. Ng, and E. C. Chang, "Live Memory Forensics of Mobile Phones," Digital Investigation, vol. 7, pp. 74–82, August 2010.

[3] J. Fernández-Boza "Fotografía digital: ventajas e inconvenientes". Rev Esp Ortod 34, pp. 335-41, 2004

[4] B. Malcolm. "El libro completo de la fotografía. Ediciones ". AKAL, 1999.

[5] S. Nagaraja, P. Schaffer, and D. Aouada, "Who clicks there: Anonymising the photographer in a camera saturated society". In Proceedings of the 10th Annual ACM Workshop on Privacy Electronic Society, pp. 13–22, 2011.

[6] T. Gloe, M. Kirchner, A. Winkler, and R. Böhme, "Can we trust digital image forensics?" in Proceedings of the 15th International Conference on Multimedia, pp. 78–86, September 2007

[7] R. Böhme and M. Kirchner, "Counter-Forensics: Attacking Image Forensic". *Digital Image Forensics*, H. T. Sencar and N. Memon, Springer-Verlag, pp. 327–366, 2013.

[8] S. Khan and A. Kulkarni. "Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform". *International Journal of Computer Applications*, vol. 6, No. 7, pp. 31-36, September 2010.

[9] B. Mahdian and S. Saic. "A Bibliography on Blind Methods for Identifying Image Forgery". *Signal Processing: Image Communication*, vol. 25, No. 6", pp. 389-399, 2010.

[10] D. King Collection, "Week in Review: A Brief History of Photo Fakery", *The New York Times*, USA, 2009.

[11] B. Laura. “The True Witness of a False Event”: Photography and Wright Morris's Fiction of the 1950s”. *Western American Literature*, vol. 33, No. 1, pp. 27-57, 2008

[12] F. Van Riper, “Manipulating Truth, Losing Credibility,” The Washington Post, USA, 2003.

[13] H. Farid. “Creating and Detecting Doctored and Virtual Images: Implications to the Child Pornography Prevention Act”. Technical Report TR2004-518, Department of Computer Science, Dartmouth College, 2004.

[14] Z. Zhang, Y. Ren, X.-J. Ping, Z.-Y. He, and S.-Z. Zhang. “A Survey on Passive-Blind Image Forgery by Doctor Method Detection”. In Proceedings of the International Conference on Machine Learning and Cybernetics, pp. 3463-3467, July 2008.

[15] J.-C. Lee. “Copy-Move Image Forgery Detection Based on Gabor Magnitude”. *Journal of Visual Communication and Image Representation*, vol. 31, pp. 320-334, 2015

[16] W.-C. Hu, J.-S. Dai, J.-S. Jian. “Effective Composite Image Detection Method Based on Feature Inconsistency of Image Components”. *Digital Signal Processing*, vol. 39, pp. 50-62, 2015

[17] A. Popescu; H. Farid. “Exposing Digital Forgeries by Detecting Traces of Resampling”. *IEEE Transactions on Signal Processing*, vol. 53, No. 2, pp. 758-767, 2005

[18] G. Muhammad; M. Hussain; G. Bebis. “Passive Copy Move Image Forgery Detection using Undecimated Dyadic Wavelet Transform”. *Digital Investigation*, vol. 9, No. 1, pp. 49-57, 2012